Pergamon

Computers Math. Applic. Vol. 36, No. 6, pp. 129–136, 1998

Printed in Great Britain
0898-1221/98 $19.00 + 0.00

PII: S0898-1221(98)00166-7

Several Extensively Tested Multiple Recursive Random Number Generators

CHIANG KAO
Graduate School of Industrial Management
National Cheng Kung University
Tainan, Taiwan, R.O.C.

HUI-CHIN TANG
Department of Industrial Engineering and Management
Cheng Shiu Junior College of Technology & Commerce
Kaohsiung, Taiwan, R.O.C.

(Received September 1997; accepted October 1997)

Abstract—The Multiple Recursive Generator (MRG) has been considered by many scholars as a very good Random Number (RN) generator. This paper applies a sequential search to identify the MRGs of orders one, two, and three which are able to produce RNs with good lattice structure in terms of the spectral value and Beyer quotient. To detect departures from local randomness and homogeneity, extensive statistical tests including runs, auto-correlation, chi-square, serial, and the sparse occupancy tests have been conducted. In approximately 19.3 billion candidates, only four MRGs, namely, (1280550, −45991), (0, 45991, 1758790), (885300443, 0, 1552858447), and (885300443, 1546795921, 598295599), have passed all the theoretical and empirical tests. Among which (0, 45991, 1758790) can be implemented efficiently by applying the approximate factoring method and is therefore most recommended. © 1998 Elsevier Science Ltd. All rights reserved.

Keywords—Multiple recursive generator, Random number, Statistics.

INTRODUCTION

Random number (RN) generators with long period that have been discussed in literature include multiple recursive generator (MRG) [1,2], Generalized Feedback Shift Register (GFSR) generator [3,4], Add-with-carry and Subtract-with-borrow (AS) generator [5], twisted-GFSR generator [6], Wichmann-Hill generator [7], and combined Tausworthe generator [8]. Tezuka [9] makes a comprehensive review of these methods. His conclusions are that all these generators are fast enough for most simulation applications and MRG, AS, and twisted-GFSR are recommended for long-period purposes. However, an important issue is how to find generators with good lattice structure in high dimensions. Furthermore, as far as portability is concerned, GFSR, twisted-GFSR, and combined Tausworthe generators depend on the programming languages being implemented. On the other hand, MRG has been considered by many scholars as a very satisfactory RN generator. As stated in Knuth [1], " ... all known evidence indicates that the result will be a very satisfactory source of RNs". Herein, we shall investigate the MRGs with good lattice structure and sound statistical properties.

A k^{th}-order MRG has the following form:

$$R_n = (a_1 R_{n-1} + \cdots + a_k R_{n-k}) \bmod m, \tag{1}$$

This research is supported by the National Science Council of the Republic of China under Contract NSC87-2213-E-006-021.

where a_i are constant multipliers in the range of $(-m+1)$ and $(m-1)$, and m is the prime modulus usually chosen to be the largest prime number that fits in a computer word. When suitable multipliers are selected, the sequence of RNs generated from (1) attains a period length $m^k - 1$ provided the seeds $R_0, \ldots, R_{k-1}$ are not all zero. Note that the first-order MRG is exactly the usual Prime Modulus Multiplicative Congruential Generator (PMMCG) which has been widely used in much computer software.

The k^{th}-order MRG can be viewed as a combination of k PMMCGs of the following form:

$$R_n = a_j R_{n-j} \bmod m, \qquad j = 1, \ldots, k. \tag{2}$$

Brown and Solomon [10] have shown that the combined generators are at least as uniformly distributed as their component generators from the majorization theory. Deng and George [11] and Deng and Chu [12] also demonstrate that the combined generators can improve the uniformity and independence properties of their individual generators. Some previous studies also reveal that the MRGs of order $k > 1$ have better properties than the PMMCG in a statistical sense. For instance, Kao *et al.* [13] study the performance of the second-order MRG with $m = 32749$, Kao and Wong [14] find some good MRGs of order two with $m = 2^{31} - 1$, and L'Ecuyer *et al.* [15] identify some MRGs of orders up to seven with good lattice structure. Nevertheless, since the statistical tests adopted are not sufficient, in particular, some stringent methods are not considered, the MRGs recommended in those studies, in fact, have flaws.

In this paper, we use a systematic method to partially search from the domain of multipliers and apply two theoretical tests to find MRGs of orders one, two, and three, which are able to produce RN streams with very good lattice structure. A set of statistical tests, including the traditional runs, auto-correlation, chi-square, and serial tests and the sparse occupancy test [16] are applied to sieve out the MRGs with very sound statistical properties. Efficiencies in implementation are also taken into consideration. In the sections that follow, we first review the lattice structure formed by the RNs produced from the MRGs. We then introduce the statistical tests to be applied to the RN streams. How to perform the theoretical and empirical tests are described next. Finally, we report the MRGs derived from this set of stringent tests. These MRGs should be suitable for practical use.

THEORETICAL TESTS

From finite field theory, the k^{th}-order MRG can produce RNs of full period $m^k - 1$ if and only if the polynomial $f(x) = x^k - a_1 x^{k-1} - \cdots - a_k$ is a primitive polynomial modulo m. Knuth [1] describes the following conditions for testing the primitivity of $f(x)$:

(i) $$(-1)^{k-1} a_k \text{ is a primitive root modulo } m, \tag{3a}$$

(ii) $$[x^r \bmod f(x)] \bmod m = (-1)^{k-1} a_k, \tag{3b}$$

(iii) $$\text{degree } \left\{ \left[x^{r/s} \bmod f(x) \right] \bmod m \right\} > 0 \text{ for each prime factor } s \text{ of } r, \tag{3c}$$

where $r = (m^k - 1)/(m-1)$. Let $\phi(\cdot)$ denote the Euler quotient function. Theoretically, there are $\phi(m^k - 1)/k$ sets of $(a_1, \ldots, a_k)$ multipliers which are able to produce full-period RNs. Coveyou and MacPherson [17] and Marsaglia [18] find that the vectors of successive numbers produced by a linear congruential generator in any dimension have a lattice structure

$$L_t = \left\{ (R_n, R_{n+1}, \ldots, R_{n+t-1})^{\top} + mz \mid n \geq 0,\ z \in Z^t \right\} \cup \{0\}. \tag{4}$$

The lattice structure implies that the points of L_t lie in parallel hyperplanes of equal distance. There are two well-known tests to evaluate the lattice structure: one is the spectral test introduced

by Coveyou and MacPherson [17] and the other is the lattice test proposed by Beyer *et al.* [19] and Marsaglia [20].

The spectral test essentially determines the maximum distance $d_t(k)$ between adjacent hyperplanes. A smaller value of $d_t(k)$ is favored because it implies smaller empty slices in L_t. Knuth [1] stresses that random sequences should pass the spectral test before they are considered to be acceptably random. Theoretically, $d_t(k)$ has a lower bound [21]:

$$d_t^*(k) = \begin{cases} \dfrac{m^{-k/t}}{r}, & \text{if } t > k, \\ \dfrac{1}{m}, & \text{if } t \leq k, \end{cases} \tag{5}$$

where r_t takes the respective values $(4/3)^{1/4}$, $2^{1/6}$, $2^{1/4}$, $2^{3/10}$, $(64/3)^{1/12}$, $2^{3/7}$, and $2^{1/2}$ for $t = 2, 3, 4, 5, 6, 7$, and 8. A figure of merit suggested by Fishman and Moore [22] is

$$S_T^*(k) = \min_{k<t\leq T} \left\{ S_t(k) \mid S_t(k) = \frac{d_t^*(k)}{d_t(k)} \right\}, \tag{6}$$

which is the worst-case measure in dimensions $k+1$ through T. The closer $S_T^*(k)$ is to unity, the better the lattice structure is of the corresponding MRG.

Geometrically, one can construct a vast number of parallelepipeds of varying volume in a lattice that includes no interior points. The presumption of the lattice test is that one prefers a lattice structure with parallelepipeds of minimal volume whose sides are close in length. A similar measure is to calculate the ratio of the lengths of the shortest to the longest basis vectors [15] from the Minkowski reduced bases [23]. This ratio $q_t(k)$ is also called Beyer quotient and a value close to 1 is preferred. As in the spectral test, the worst-case measure

$$Q_T^*(k) = \min_{k<t\leq T} \{q_t(k)\} \tag{7}$$

is adopted as a figure of merit.

EMPIRICAL TESTS

In general, theoretical tests examine global randomness. However, since most of the time, only a small fraction of the whole cycle of RNs will be used in simulation studies, the local randomness is also very important. As indicated by Knuth [1], although the spectral test is a very powerful test, the empirical tests still cannot be eliminated. The local evaluation is usually performed by statistically testing subsequences of RNs produced from a generator to see how close those numbers resemble iid uniform random variates. Some famous statistical tests are the runs and auto-correlation tests for testing independence and the chi-square and serial tests for testing uniformity in different dimensions. Several empirical studies [13,14,22,24] reveal that these classical tests are rather easy for the RN generators to pass. Marsaglia and Zaman [16] have devised a type of test which is very effective and convincing for assessing both uniformity and independence in the output of a RN generator. The basic idea is to count the frequency of all the possible t-digit string patterns in a random sequence. As the memory requirement is concerned, Marsaglia and Zaman [16] change the test to counting the presence or absence of each t-digit string pattern instead of counting frequency, and term the test Sparse Occupancy (SO) test.

Marsaglia and Zaman [16] suggest four SO tests, namely, Overlapping-Pairs-SO (OPSO), Overlapping-Triples-SO (OTSO), Overlapping-Quadruples-SO (OQSO), and DNA tests. In the OPSO test, the first ten bits or any particular ten bits of an integer produced by the MRG determines the string pattern. For most applications, the leading bits of a RN generator are the most important. Thus, it is more appropriate to test the first ten bits. For overlapping

two-tuples of successive RNs, there are 2^{10} string patterns. The number of missing two-tuple string patterns should be approximately normal with $\mu = 141909$ and $\sigma = 290.26$ in a sample of 2^{21} RNs [16]. Similarly, in the OTSO, OQSO, and DNA tests, we look at the first six, five, and two bits, respectively, of an integer. The number of missing three-tuple, four-tuple, and ten-tuple string patterns in these three tests are approximately normal with means 87.9393, 141909.33, 141910.5378 and standard deviations 9.37, 290.33, 290 in a sequence of 2^{21} RNs. Marsaglia and Zaman [16] stress that a good RN generator should pass all these tests.

METHODS

In this study, the modulus considered is the very popular one $m = 2^{31} - 1$. For this modulus, the number of $(a_1, \ldots, a_k)$ multipliers which are able to produce full-period RNs are 5.346E8, 5.740E17, and 8.218E26 for first-order, second-order, and third-order MRGs, respectively. The number of all possible $(a_1, \ldots, a_k)$ combinations for these three orders are $(2^{31} - 1) \cong 2.15E9$, $(2^{31} - 1)^2 \cong 4.61E18$, and $(2^{31} - 1)^3 \cong 9.9E27$, respectively. It is hardly possible to examine all sets of multipliers. According to the idea of Brown and Solomon [10], Deng and George [11], or Deng and Chu [12], if one of the component generators in a combined generator has good statistical properties, then the combined generator has better statistical properties. Therefore, one systematical and considerably effective way for generating good $(a_1, \ldots, a_k)$ multipliers is to generate $(a_1), (a_1, a_2), \ldots, (a_1, \ldots, a_k)$, sequentially. Initially, an exhaustive search for the best multiplier for the first-order MRG, i.e., PMMCG, in terms of the spectral value is conducted. Then, we fix a_1 at the value just found, and search for a_2 in the range of $(1, m - 1)$ to result in a conceivably good MRG of order two. Subsequently, we use MRG of order i to generate MRG of order $i + 1$, $i = 2, 3, \ldots, k - 1$. In the searching process, condition (3) must be satisfied. This method can also be applied in a backward manner. That is, in generating good $(a_1, \ldots, a_k)$ multipliers, we fix a_k at the value of the best multiplier for the first-order MRG and search for a_{k-1} in the range of $(1, m - 1)$ to result in a good MRG of order two. Then, we search for a_{k-2}, a_{k-3}, and so forth in sequence until a_1 is found. This sequential search method reduces the domain of multipliers for searching from $(m - 1)^k$ to $k(m - 1)$ for the k^{th}-order MRG.

In (1), computing $(a_i R_{n-i} \bmod m)$ accounts for most of the computation time, and the speed of a generator is approximately inversely proportional to the number of such operations [15]. Obviously, MRG with fewer terms in the recursive relationship is desired from the viewpoint of computation efficiency. Therefore, MRGs of order k with $h < k$ terms are also considered in this study, although Kao and Tang [25] have shown that these kinds of MRGs have less satisfactory lattice structure than that of the regular k^{th}-order MRG.

Another way to acquire computational efficiency is to require the multiplier a_i to satisfy

$$|a_i (m \bmod a_i)| < m, \tag{8}$$

so that the approximate factoring method [15,26,27] can be utilized to efficiently calculate $(a_i R_{n-i} \bmod m)$. This idea is also implemented in this study.

In sum, the procedure of this study is to apply the sequential method, both forward and backward, to find full-period MRGs of orders one, two, and three. Two aforementioned efficient implementations are also considered. In each case, 20 sets of multipliers which have the largest spectral values $S_T(k)$ for the RNs produced are selected to calculate the Beyer quotient and to conduct the empirical tests. The dimension T considered in this study is eight as suggested by Knuth [1] and Riply [28].

In the empirical tests, a two-level test is conducted to increase the power [29]. Specifically, every test is repeated 1,000 times on consecutive subsequences of 200,000 numbers each, taking $(R_0, R_1, R_2) = (1, 1, 1)$ as the seed. The empirical distributions of those 1,000 statistics are then compared to the corresponding theoretical distributions via the standard Kolmogorov-Smirnov

goodness-of-fit test. The auto-correlation test is conducted for lags 1 through 3. For the chi-square test, the number of intervals used is 500 as calculated from the Mann-Wald formula [30]. The serial test is conducted for dimensions two and three, and the number of intervals used are 20^2 and 7^3, respectively.

RESULTS

The whole computation is conducted on a DEC Alpha computer with programs coded in C. The sequential search together with the theoretical tests take about 1638 CPU hours. Approximately 19.3 billion multipliers have been examined. Another 1977 CPU hours are used for the two-level empirical tests. After these extensive tests, only four sets of multipliers have left, in that the significance level is set at 5%. They are (1280550, −45991), (0, 45991, 1758790), (885300443, 0, 1552858447), and (885300443, 1546795921, 598295599), in that the first two sets can be implemented efficiently by applying the approximate factoring method. Table 1 lists the spectral values, Beyer quotients, and the p-values of different statistical tests of these four MRGs.

Table 1. Results of the statistical tests for the four MRGs derived in this study.

Tests	1280550 −45991	0 45991 1758790	885300443 0 1552858447	885300443 1546795921 598295599
$S_8^*(k)$	0.65765	0.14741	0.15628	0.76262
$Q_8^*(k)$	0.56100	0.00070	0.00071	0.72723
Runs	0.10230	0.31963	0.11477	0.58159
Auto-correlation 1	0.37453	0.56000	0.34201	0.17871
Auto-correlation 2	0.61134	0.44626	0.23292	0.18815
Auto-correlation 3	0.27742	0.70581	0.18669	0.26713
Chi-square	0.20458	0.58627	0.19541	0.11427
Serial 2	0.43759	0.28032	0.19808	0.27415
Serial 3	0.18740	0.06464	0.76233	0.57032
OPSO	0.25980	0.20605	0.15133	0.27705
OTSO	0.09332	0.05600	0.10456	0.08140
OQSO	0.30191	0.22337	0.09464	0.47281
DNA	0.06415	0.06838	0.06341	0.07948

Table 2. Results of the statistical tests for the seven MRGs found by L'Ecuyer *et al.* [15].

Test	41358	1385320287	46325 1084587	1498809829 1160990996	65338 0 64636	1476728729 0 1155643113	2021422057 1826992351 1977753457
$S_8^*(k)$	0.60194	0.66367	0.58103	0.64358	0.00775	0.13778	0.64974
$Q_8^*(k)$	0.62087	0.65373	0.35748	0.66843	0.00004	0.00075	0.70520
Runs	0.29512	0.11935	0.04918*	0.32158	0.13943	0.16222	0.02468*
Auto. 1	0.44577	0.67099	0.31992	0.29976	0.07911	0.03749*	0.28531
Auto. 2	0.22467	0.21345	0.00870*	0.19011	0.56497	0.01871*	0.57650
Auto. 3	0.41932	0.50962	0.53739	0.41696	0.26630	0.08333	0.12715
Chi-square	0.06669	0.30161	0.04507*	0.35965	0.24661	0.02301*	0.23936
Serial 2	0.34657	0.37785	0.58315	0.09794	0.53081	0.12179	0.40291
Serial 3	0.58279	0.40249	0.01075*	0.18279	0.47394	0.32705	0.08785
OPSO	0.00000*	0.00000*	0.37209	0.30984	0.30675	0.37306	0.06320
OTSO	0.00974*	0.04029*	0.04746*	0.07409	0.08522	0.00004*	0.08522
OQSO	0.00000*	0.00000*	0.24288	0.14243	0.21211	0.22332	0.38343
DNA	0.00000*	0.00000*	0.00021*	0.01558*	0.00422*	0.00152*	0.01692*

*Significant at the 5% level.

Table 3. The $d_t(k)$ values for the MRGs of this study and L'Ecuyer *et al.* [15].

MRG	$d_2(k)$	$d_3(k)$	$d_4(k)$	$d_5(k)$	$d_6(k)$	$d_7(k)$	$d_8(k)$
(1280550, −45991)	4.6566E − 10	7.8041E − 7	2.7028E − 5	2.0123E − 4	7.7376E − 4	2.1816E − 3	4.9947E − 3
(0, 45991, 1758790)	4.6566E − 10	4.6566E − 10	5.7183E − 7	5.0358E − 6	2.2214E − 5	9.1623E − 5	5.1299E − 4
(885300443, 0, 1552858447)	4.6566E − 10	4.6566E − 10	5.3938E − 7	5.7952E − 6	2.6930E − 5	1.1507E − 4	3.3672E − 4
(885300443, 1546795921, 598295599)	4.6566E − 10	4.6566E − 10	1.0154E − 7	2.5471E − 6	2.1676E − 5	9.5151E − 5	2.9356E − 4
(41358)	2.4179E − 5	9.8113E − 4	5.5726E − 3	1.5079E − 2	3.2427E − 2	5.0252E − 2	8.0064E − 2
(1385320287)	2.6171E − 5	8.8049E − 4	5.4136E − 3	1.3664E − 2	2.7886E − 2	5.1988E − 2	7.1247E − 2
(46325, 1084587)	4.6566E − 10	9.2117E − 7	2.5782E − 5	2.4224E − 4	8.1432E − 4	2.3466E − 3	5.0111E − 3
(1498809829, 1160990996)	4.6566E − 10	6.3493E − 7	2.4103E − 5	1.9482E − 4	8.4075E − 4	2.4896E − 3	4.8563E − 3
(65338, 0, 64636	4.6566E − 10	4.6566E − 10	1.1088E − 5	1.0881E − 5	3.3581E − 5	1.0373E − 4	3.6611E − 4
(1476728729, 0, 1155643113)	4.6566E − 10	4.6566E − 10	6.1180E − 7	2.7210E − 6	2.7449E − 5	9.7086E − 5	3.0853E − 4
(2021422057, 1826992351, 1977753457)	4.6566E − 10	4.6566E − 10	1.1012E − 7	2.7970E − 6	2.2412E − 5	1.0578E − 4	3.4457E − 4

The spectral values of (0, 45991, 1758790) and (885300443, 0, 1552858447) are relatively small compared with the other third-order MRG (885300443, 1546795921, 598295599). The reason is that $d_{k+1}(k)$ of the k^{th}-order MRG with $h < k$ terms is equal to $d_{h+1}(h)$ of the h^{th}-order MRG with h terms [25]. Therefore, one should use $d^*_{h+1}(h)$ instead of $d^*_{k+1}(k)$ to calculate $S_{k+1}(k)$ for the k^{th}-order MRG with h terms. If this is taken into account, then the spectral value of the two-term third-order MRGs will increase to a very large extent. The reason for smaller values in the Beyer quotient for these two MRGs is similar.

L'Ecuyer *et al.* [15] conduct a random search to find some MRGs with good lattice structure in terms of the Beyer quotient with T as large as twenty. Since the MRGs derived in this study are based on the spectral value rather than the Beyer quotient, these two sets of MRGs are incomparable. However, when we apply the empirical tests to the MRGs found by L'Ecuyer *et al.*, some interesting results are observed. Table 2 contains the seven MRGs of orders one, two, and three found by L'Ecuyer *et al.* [15]. By applying the same two-level statistical tests to conform with that of Table 1, the p-values of every test are calculated. Three MRGs, namely (46325, 1084587), (1476728729, 0, 1155643113), and (2021422057, 1826992351, 1977753457), have failed in some of the traditional tests (runs, auto-correlation, chi-square, and serial) at the 5% significance level. All seven of the MRGs have failed in certain SO tests; notably, every MRG has failed in the DNA test. In other words, although those seven MRGs have very good lattice structure, the local randomness is not acceptable.

To grasp some idea about the lattice structure of the MRGs of this study and that of L'Ecuyer *et al.* [15], we have calculated their $d_t(k)$ values as shown in Table 3. In general, the third-order MRGs have the smallest distance between adjacent hyperplanes in all dimensions, whereas the first-order MRGs have the largest distance.

CONCLUSION

In simulation studies, the quality of the RN generator adopted has a major effect on the results derived. An ideal RN generator should possess at least the properties of long period, good lattice structure, and sound statistical properties [31]. With regard to period, the opinion of L'Ecuyer [29] is that any generator with period shorter than 2^{50} is not suitable for practical use. For $m = 2^{31} - 1$, the second- and third-order MRGs have period lengths of around 2^{62} and 2^{93}, respectively, which obviously meet the minimal requirement of L'Ecuyer.

The lattice structures of the RNs produced by the MRGs are examined by the spectral test and the lattice test. Owing to the astronical number of candidate multipliers, a sequential search is conducted, and 360 MRGs with very good lattice structure are sieved out. After the extensive empirical tests, including the traditional runs, auto-correlation, chi-square, and serial tests and the stringent SO tests, only four MRGs have left, viz. (1280550, −45991), (0, 45991, 1758790), (885300443, 0, 1552858447), and (885300443, 1546795921, 598295599). These MRGs have both good global and local randomness properties. Notably, none of these MRGs is of the first order.

Of the four MRGs derived in this study, (1280550, − 45991) and (0, 45991, 1758790) are more efficient because the approximate factoring method can be applied in generating RNs. Since (0, 45991, 1758790) is a third-order MRG whose period and lattice structure are better than the second-order MRG (1280550, −45991), it is, therefore, an ideal RN genarator for large-scale simulation studies.

REFERENCES

1. D.E. Knuth, *The Art of Computer Programming, Volume 2: Semi-Numerical Algorithms*, Second edition, Addison-Wesley, Reading, MA, (1981).
2. P. L'Ecuyer, Random numbers for simulation, *Commun. of the ACM* **33**, 85–97 (1990).
3. T.G. Lewis and W.H. Payne, Generalized feedback shift register pseudorandom number algorithms, *J. of the ACM* **20**, 456–468 (1973).

4. M. Fushimi and S. Tezuka, The k-distribution of generalized feedback shift register pseudorandom numbers, *Commun. of the ACM* **26**, 519–523 (1983).
5. G. Marsaglia and A. Zaman, A new class of random number generators, *The Annals of Applied Probability* **1**, 462–480 (1991).
6. M. Matsumoto and Y. Kurita, Twisted GFSR generators, *ACM Trans. on Modeling and Computer Simu.* **2**, 179–194 (1992).
7. B.A. Wichmann and I.D. Hill, An efficient and portable pseudorandom number generator, *Applied Statistics* **31**, 188–190 (1982).
8. S. Tezuka and P. L'Ecuyer, Efficient and portable combined Tausworthe random number generators, *ACM Trans. on Modeling and Computer Simu.* **1**, 99–112 (1991).
9. S. Tezuka, A unified view of long-period random number generators, *J. of the Opnl. Res. Society,* Japan **37**, 211–227 (1994).
10. M. Brown and H. Solomon, On combining pseudorandom number generators, *Annals of Statistics* **3**, 691–695 (1979).
11. L.Y. Deng and E.O. George, Generation of uniform variates from several nearly uniformly distributed variables, *Commun. in Stat.* **B19**, 145–154 (1990).
12. L.Y. Deng and Y.C. Chu, Combining random number generators, In *Proceedings of the 1991 Winter Simulation Conference*, pp. 1043–1046, (1991).
13. C. Kao, J.Y. Wong and N.J. Liu, Multiplicative congruential random number generator of order two with modulus 32749, *Int. J. Computer Simul.* **6**, 513–525 (1996).
14. C. Kao and J.Y. Wong, Random number generators with long period and sound statistical properties, *Computers Math. Applic.* **36** (3), 113–121 (1998).
15. P. L'Ecuyer, F. Blouin and R. Couture, A search for good multiple recursive random number generators, *ACM Trans. on Modeling and Computer Simu.* **3**, 87–98 (1993).
16. G. Marsaglia and A. Zaman, Monkey tests for random number generator, *Computers Math. Applic.* **26** (9), 1–10 (1993).
17. R.R. Coveyou and R.D. MacPherson, Fourier analysis of uniform random number generators, *J. of the ACM* **14**, 100–119 (1967).
18. G. Marsaglia, Random numbers fall mainly in the planes, *Proc. of the Nat. Acad. Sci.* **60**, 25–28 (1968).
19. W.A. Beyer, R.B. Roof and D. Williamson, A lattice structure of multiplicative congruential pseudo-random vectors, *Math. Comput.* **25**, 345–363 (1971).
20. G. Marsaglia, The structure of linear congruential sequences, In *Applications of Number Theory to Numerical Analysis*, (Edited by S.K. Zeremba), pp. 249–285, Academic Press, New York, (1972).
21. J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, New York, (1959).
22. G.S. Fishman and L.R. Moore, III, An exhaustive analysis of multiplicative congruential random number generators with modulus 231-1, *SIAM J. on Sci. Stat. Comput.* **7**, 24–45 (1986).
23. L. Afflerbach and H. Grothe, Calculation of Minkowski-reduced lattice bases, *Computing* **35**, 269–276 (1985).
24. C. Kao and J.Y. Wong, Several extensively tested random number generators, *Computers Ops. Res.* **21**, 1035–1039 (1994).
25. C. Kao and H.C. Tang, Upper bounds in spectral test for multiple recursive random number generators with missing terms, *Computers Math. Applic.* **33** (4), 119–125 (1997).
26. P. L'Ecuyer, Efficient and portable combined random number generators, *Commun. of the ACM* **31**, 742–774 (1988).
27. S.K. Park and K.W. Miller, Random number generators: Good ones are hard to find, *Commun. of the ACM* **31**, 1192–1201 (1988).
28. B.D. Ripley, Thoughts on pseudorandom number generators, *J. Computers and Applied Math.* **31**, 153–163 (1990).
29. P. L'Ecuyer, Testing random number generators, In *Proceedings of the 1992 Winter Simulation Conference*, pp. 305–313, (1992).
30. M.A. Hamdan, The number and width of classes in the chi-square test, *J. American Stat. Association* **58**, 678–689 (1963).
31. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, (1992).